Order Code RS20037
Updated October 6, 2000

"Junk E-mail": An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam")

Marcia S. Smith
Specialist in Aerospace and Telecommunications Policy
Resources, Science, and Industry Division

Summary

Unsolicited commercial e-mail (UCE), also called "spam" or "junk e-mail," aggravates many computer users. Not only can it be a nuisance, but its cost may be passed on to consumers through higher charges from Internet service providers who must upgrade their systems to handle the traffic. Proponents of UCE insist it is a legitimate marketing technique and protected by the First Amendment. Legislation to place limits on UCE was considered by the 105th Congress, but did not pass. Debate has continued in the 106th Congress, and the House passed H.R. 3113 on July 18,2000. Several other bills also are pending. This report will be updated.

Overview

One aspect of increased use of the Internet for electronic mail (e-mail) has been the advent of unsolicited advertising, also called "unsolicited commercial e-mail (UCE)," "unsolicited bulk e-mail," "junk e-mail, "or "spam."[1] Issues involved in the debate are reviewed in *Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email* [http://www.cdt.org/spam].

In 1991, Congress passed the Telephone Consumer Protection Act (P.L. 102-243) that prohibits, *inter alia*, unsolicited advertising via facsimile machines, or "junk fax" (see CRS Report 98-514, *Telemarketing Fraud: Congressional Efforts to Protect Consumers*). Many think there should be an analogous law for computers, or at least

[1] The origin of the term spam for unsolicited commercial e-mail was recounted in *Computerworld*, April 5, 1999, p. 70: "It all started in early Internet chat rooms and interactive fantasy games where someone repeating the same sentence or comment was said to be making a 'spam.' The term referred to a Monty Python's Flying Circus scene in which actors keep saying 'Spam, Spam, Spam and Spam' when reading options from a menu."

some method for letting a consumer know before opening an e-mail message whether or not it is unsolicited advertising and how to direct the sender to cease transmission of such messages. At a November 3, 1999 hearing of the House Commerce telecommunications subcommittee, a representative of SBC Internet Services, a subsidiary of SBC Communications, Inc., stated that 35% of all the e-mail transmitted over SBC's Internet systems in its Pacific Bell and Southwestern Bell regions is UCE.

Opponents of junk e-mail such as the Coalition Against Unsolicited Commercial Email (CAUCE) [http://www.cause.org] argue that not only is junk e-mail annoying, but its cost is borne by consumers, not marketers. Consumers reportedly are charged higher fees by Internet service providers that must invest resources to upgrade equipment to manage the high volume of e-mail, deal with customer complaints, and mount legal challenges to junk e-mailers. According to *Internet Week (*May 4, 1998), $2 of each customer's monthly bill is attributable to spam [http://www.techweb.com/se/directlink.cgi?INW19980504S0003]. Consumers also may incur costs for the time spent reading and/or deleting such e-mail. Some want to prevent bulk e-mailers from sending messages to anyone with whom they do not have an established business relationship, treating junk e-mail the same way as junk fax.

Proponents of unsolicited commercial e-mail argue that it is a valid method of advertising. The Direct Marketing Association (DMA), for example, argues that instead of banning unsolicited commercial e-mail, individuals should be given the opportunity to notify the sender of the message that they want to be removed from its mailing list — or "opt-out." Hoping to demonstrate that self regulation can work, in January 2000, the Direct Marketing Association launched a new service, the E-mail Preference Service, where consumers who wish to opt out of receiving UCE can register themselves at a DMA Web site [http://www.e-mps.org]. DMA members sending UCE must check their lists of intended recipients and delete those who have opted out via that Web site. Critics argue that most spam does not come from DMA members, so the plan is insufficient.

To date, the issue of restraining junk e-mail has been fought primarily over the Internet or in the courts. Some Internet service providers will return junk e-mail to its origin, and groups opposed to junk e-mail will send blasts of e-mail to a mass e-mail company, disrupting the company's computer systems. Filtering software also is available to screen out e-mail based on keywords or return addresses. Knowing this, mass e-mailers may avoid certain keywords or continually change addresses to foil the software, however. In the courts, Internet service providers with unhappy customers and businesses that believe their reputations have been tarnished by misrepresentations in junk e-mail have brought suit against mass e-mailers.

Consumers may file a complaint about spam with the Federal Trade Commission (FTC) by visiting the FTC Web site [http://www.ftc.gov] and scrolling down to "complaint form" at the bottom of the page. The offending spam also may be forwarded to the FTC (UCE@ftc.gov) to assist the FTC in monitoring UCE trends and developments. The FTC has three consumer publications that are available on the FTC Web site [http://www.ftc.gov/opa/1999/9911/spam.htm].

Some unsolicited e-mail either contains indecent material or provides links to other sites where indecent material is available. Thus, controls over junk e-mail have also arisen in the context of protecting children from unsuitable material. In October 1997, AOL filed

suit to prevent a company that sends unsolicited e-mails offering "cyberstrippers" from sending e-mail to AOL subscribers. The company, Over the Air Equipment, agreed on December 18, 1997 to drop its challenge to a preliminary injunction barring it from sending such advertisements to AOL subscribers (Reuters, December 18, 1997, 11:57 AET).

Other spam involves fraud, which also may involve links to adult entertainment services. The FTC reported at the November 3, 1999 House Commerce committee hearing that it had brought 17 actions against schemes that used spam as part of their operation. As an example, the FTC witness cited a scheme in which consumers would receive a spam message that an order had been received and processed and their credit cards would be billed, and to call a specified telephone number with any questions. Unknown to the consumers, the telephone number was in Dominica, West Indies. When the consumers called to speak to a company representative, they instead were connected to an adult entertainment audiotext service and then were billed for international long-distance calls. The FTC reported that it had approved a stipulated final order in this case (FTC v. Benoit) and settlement was awaiting approval by a federal district court.

State Action

Although the U.S. Congress has not passed a law addressing junk e-mail, several states have passed or considered such legislation. According to the National Conference of State Legislatures, as of March 2000, 15 states (California, Connecticut, Delaware, Illinois, Iowa, Louisiana, Nevada, North Carolina, Oklahoma, Rhode Island, Tennessee, Vermont, Virginia, Washington, and West Virginia) have enacted such laws and 16 introduced spam legislation in their 2000 sessions.[2]

105th Congress Activity

Although the House and Senate each passed legislation addressing the unsolicited commercial e-mail issue, no bill ultimately cleared the 105th Congress. The Senate had adopted a Murkowski-Torricelli amendment to S. 1618, the Anti-slamming[3] Amendments Act, that follows the "opt-out" philosophy and reflected provisions in S. 771 (Murkowski) and S. 875 (Torricelli). The language would have required senders of commercial e-mail to clearly identify in the subject line of the message that it was an advertisement, required Internet service providers to make software available to their subscribers to block such e-mail, and prohibited sending e-mail to anyone who had asked not to receive such mail.

Similar language was included in the House version of the Anti-slamming bill, H.R. 3888 (Tauzin), marked up by the House Commerce Telecommunications Subcommittee on August 6, 1998. Concerns were raised by several subcommittee members during the markup, however, that the language might infringe on First Amendment rights, and commented that they wanted more information before proceeding with the bill because of

---

[2]National Conference of State Legislatures (Denver, CO office). States Enact Anti-Spam Legislation. March 1, 2000.

[3]"Slamming" is the unauthorized change of someone's long distance telephone service provider. See CRS Issue Brief IB98027.

that and other issues. A very different version was adopted during full committee markup on September 24. As reported from the full committee (H.Rept. 105-801), the bill included only a sense of Congress statement that industry should self-regulate in this area. The bill passed the House on October 12, but differences between the House and Senate on this and other issues could not be resolved before Congress adjourned.

106th Congress Activity

Spam continues to be a major area of concern to Internet users. The House passed H.R. 3113 on July 18, 2000; several other bills also are pending, as summarized below.

Table 1: Related 106th Congress Legislation

Bill	Summary
H.R. 1685 (Boucher/ Goodlatte)	**Internet Growth and Development Act**. Referred to Committees on Commerce and Judiciary. Section 201 prohibits registered users, persons, or other entities from using or causing to be used an e-mail service provider's equipment for transmitting UCE in violation of that e-mail service provider's policy against such activities.
H.R. 1686 (Goodlatte/ Boucher)	**Internet Freedom Act**. Referred to Committees on Judiciary and Commerce. Section 104 makes it a crime to intentionally and without authorization initiate the transmission of UCE to a protected computer knowing that the message falsifies certain identifying information, or to sell or distribute a computer program that is specially designed to conceal the source or routing of UCE, otherwise has limited commercially significant purpose, or is marketed for that use.
H.R. 1910 (G. Green)	**E-mail User Protection Act**. Referred to Committees on Commerce and Judiciary. Makes it unlawful to initiate transmission of UCE containing certain false identifying information, to fail to comply with a request to cease sending such messages, or to create, sell, or distribute computer software primarily designed to create certain false identifying information on an e-mail message; gives rights of action and recovery of civil damages to interactive computer services and recipients of such e-mail who are adversely affected. *Representative Green also co-sponsored the version of H.R. 3113 that passed the House July 18, 2000; see below.*
H.R. 2162 (G. Miller)	**Can Spam Act**. Referred to Committees on Commerce and Judiciary. *Inter alia*, prohibits persons from using or causing to be used equipment of an e-mail service provider for transmitting UCE in violation of a posted policy of that e-mail service provider.
H.R. 3024 (C. Smith)	**Netizens Protection Act**. Referred to Committee on Commerce. Makes it unlawful to initiate or cause to be initiated UCE if the message does not include the name, physical address, and e-mail address of the person initiating the transmission; does not provide an electronic method to opt-out; or is part of a bulk transmission and includes information in the subject line that is false or misleading about the body of the message. Does not preempt state laws. Provides for persons adversely affected to bring civil actions. Requires interactive computer service providers to

Bill	Summary
	make their policies on UCE available to their customers and prohibits those customers from using the companies' equipment or facilities for bulk UCE transmission if the policy prohibits it. Interactive computer service providers that take action to prevent receipt of UCE are not liable for harm resulting from failure to prevent such receipt.
H.R. 3113 (Wilson) PASSED THE HOUSE JULY 18, 2000	**Unsolicited Electronic Mail Act**. *As passed by the House*. Makes it unlawful to initiate transmission of any commercial e-mail to anyone in the U.S. unless it has a valid and conspicuous reply e-mail address to which recipient can opt-out. If a person opts-out, unlawful to initiate transmission of unsolicited commercial e-mail (UCE, defined as commercial e-mail sent to someone with whom the initiator has no pre-existing business relationship) to that person after reasonable time to remove person from distribution list. Opt-out notification terminates pre-existing business relationship for purposes of the Act. Makes it unlawful to initiate UCE to anyone in the U.S. unless the message provides clear and conspicuous identification that the message is UCE and opt-out is available. Makes it unlawful to initiate the transmission of UCE in violation of an ISP policy if the policy: explicitly provides that compliance is a condition of use of the ISP's equipment, is publicly available on its Web site or made available in accordance with a technological standard adopted by an appropriate Internet standards setting body, and provides an opt-out option for its subscribers if it requires compensation for the transmission of UCE and the subscriber has not agreed to receive UCE in exchange for discounted or free Internet access service. ISPs not liable for actions taken in good faith to block UCE. If ISP facilities are used only to handle, transmit, retransmit, or relay UCE transmitted in violation of Act, ISP not liable for harm caused unless it had actual knowledge that transmission was prohibited. FTC shall send notice of alleged violation to initiator of UCE if so notified by a recipient of UCE or ISP, or has other reason to believe violation has occurred. Notice shall *inter alia* direct initiator to cease, and to delete names and e-mail addresses of recipient and, if requested, recipient's children under 18, from all its mailing lists and initiator may not sell or otherwise provide those addresses to others. Gives FTC enforcement authority and U.S. district courts upon application by the Attorney General may issue orders commanding compliance. Recipients and ISPs may sue to recover actual monetary loss, or $500 per violation up to $50,000, whichever is greater, and court may increase the amount up to three times for willful, knowing, or repeated violators. Court may protect trade secrets. Amends 18 U.S.C. 1030 to make it a crime to intentionally initiate the transmission of UCE to a protected computer knowing that the message falsifies certain identifying information. State and local governments may not impose civil liabilities inconsistent with the Act, but Act does not preempt civil remedies under State trespass or contract law or any laws relating to computer fraud or abuse arising from UCE. FTC to prepare report on effectiveness and enforcement of the Act.
H.R. 5300 (Holt)	**Wireless Telephone Spam Protection Act**. Prohibits transmitting unsolicited commercial advertisements via text, graphic, and image messaging systems for wireless telephones. (Commerce)

Bill	Summary
S. 759 (Murkowski)	**Inbox Privacy Act**. Referred to Committee on Commerce. Requires "opt-in/opt-out" options for consumers and domain name owners; requires transmitters of UCE to include specified information in the body of a UCE message; allows the Federal Trade Commission (FTC) to prescribe rules for defining and prohibiting deceptive acts and practices connected with sales of goods or services over the Internet; allows states to bring civil actions on behalf of their residents if they are adversely affected by UCE, but they must notify the FTC and the FTC may intervene; allows ISPs or interactive computer service providers to bring civil actions for violation of the Act; and preempts any state or local laws regarding the transmission or receipt of commercial e-mail.
S. 2448 (Hatch)	**Internet Integrity and Critical Infrastructure Protection Act**. Referred to Committee on the Judiciary. As introduced, included section prohibiting transmittal of UCE to protected computers containing false identifying information, but ***this section was deleted*** in substitute amendment adopted by committee October 5, 2000.
S. 2542 (Burns)	**Controlling the Assault of Non-Solicited Pornography and Marketing Act**. Referred to Committee on Commerce. Makes it unlawful to initiate transmission of UCE to anyone in the United States without providing legitimate return e-mail address for opting-out, to include false or misleading e-mail transmission address or routing information, or to sell or distribute software for those purposes; allows ISPs to decline to transmit UCE without compensation and ISPs are held harmless for actions taken in good faith to block UCE; makes it unlawful to use or disclose domain name registry data if it violates policies of that registrar posted on its Web site and it is used for UCE; directs FTC, when notified by a recipient or ISP of a violation of the Act, to send notice directing that person to stop; establishes related authorities of FTC, states, and U.S. district courts; and directs FTC to conduct 18 month study on effectiveness of this Act, enforcement actions taken under this Act, and needed modifications, if any.

H.R. 3113 was marked up by subcommittee on March 23, 2000. It was ordered reported from full committee on June 14 after an amendment in the nature of a substitute, sponsored by Representatives Wilson and Green, was adopted. The report was filed on June 26 (H.Rept. 106-700). H.R. 3113 passed the House (427-1) on July 18, 2000. The version of the bill brought to the House floor contained changes to the committee-reported version. *Inter alia*, in the new version (as printed in the *Congressional Record*, July 18, 2000, pp. H 6369-6371) the section that made it unlawful to send UCE unless it has a valid and conspicuously displayed e-mail address to which a person can opt-out now applies to all commercial e-mail, not just unsolicited commercial e-mail. Sections making it unlawful to take any action that causes Internet routing information to be inaccurate, and authorizing Internet service providers to enforce their UCE policies, were deleted. Language was added making it a crime to initiate the transmission of UCE to a protected computer (not defined in H.R. 3113, but that section amends 18 U.S.C. 1030, which defines protected computers essentially as computers for the use of a financial institution or the U.S. government, or used in interstate or foreign commerce or communication). The added language is similar but not identical to language in H.R. 1686.